VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Počítačové komunikace a sítě 2. projekt.

ARP Scanner

23. dubna 2017 Radek Mojžíš

Obsah

1 ARP scanner

Následuje stručný výtah informací z nastudované literatury.

1.1 K čemu ARP slouží

The Address Resolution Protocol (zkratka ARP) je komunikační protokol sloužící k spojení adresy síťové úrovně s adresou fyzické úrovně. Neboli mapování síťových adres (např. IPv4 adres) na fyzické adresy (také známy jako MAC adresy). [1]

1.2 Základní princip ARP scanneru

Na broadcastovou adresu dané podsítě se pošle ARP zpráva s dotazem, „kdo“ má dotazovanou adresu síťového protokolu (dále „IP adresu“). Dále se čeká na příchozí ARP zprávy s odpovědí na dotaz. Toto se provede pro každou požadovanou IP adresu.

1.3 Struktura ARP zprávy

Hlavička ARP zprávy je 26 bytů tlouhá a obsahuje následující informace. [1]

Byte 0-1: Typ systémového protokolu (př: Ethernet je 1).

Byte 2-3: Typ síťového protokolu (př: IPv4 je 0x0800).

Byte 4: Délka (v bytech) hardwarové adresy (Pro Ethernet 6).

Byte 5: Délka (v bytech) adresy protokolové úrovně (pro IPv4 4).

Byte 6-7: Operace (pro žádost 1, pro odpověď 2).

Byte 8-13: Hardwarová adresa odesilatele.

Byte 14-17: IP adresa odesilatele.

Byte 18-23: Hwrdwarová adresa příjemce (v ARP žádosti ignorováno).

Byte 24-27: IP adresa příjemce.

2 Implementace

Následuje stručný popis implementace.

2.1 Návrh

Úloha byla řešena v jazyce C, neboť nejde onijak veliký projekt a také proto, že by se v něm velmi často při práci s RAW sockety v c++ používal „reinterpret cast“, což by značně přidalo na nečitelnosti kódu.

2.2 Popis činnosti

Program v pořadí dělá následující operace.

2.2.1 Načtění argumentů

Nejprve se načtou vstupní argumenty, zkontroluje se jejich počet a uloží se jméno požadovaného rozhraní.

2.2.2 Inicializace socketu

Komunikační socket se vytváří voláním funkce socket()
`socket(AF_PACKET, SOCK_RAW, htons(ETH_P_ALL));`.

2.2.3 Získávání informací o rozhraní

Následně se pomocí série volání funkce `ioctl()` načtou potřebné **informace o požadovaném rozhraní**, zejména jsou to informace jako je **MAC adresa** rozhraní, **IP adresa** v dané síti a **maska podsítě**. [2]

2.2.4 Vytvoření ethernetového rámce

Dále se do bytového pole vytvoří ethernetový rámec. Rámec má na začátku Ethernetovou hlavičku a pokračuje potom samotnou ARP žádostí. Na konci je doplněn do 64 bytů nulami, neboť cokoliv menšího, než 64 bytů je bráno jako fragment komunikace a „zahazuje“ se.
Ethernetová hlavička má 14 bytů a obsahuje hardwarovou adresu příjemce (6 bytů, pro broadcast je to `0xffff.ffff.ffff`) a MAC adresu odesilatele (6 bytová MAC adresa rozhraní) a 2 byty na protokolový typ, což je pro ARP `0x0806`.
Arp hlavičku plním pomocí datové struktury s nastavením `__atribute__((packed))`, pro zrušení implicitního zarovnávání paměti.

2.2.5 Odesílání žádosti

Po sestavení žádosti se program rozdělí na dvě vlákna. První vlákno odesílá ARP žádosti na každou možnou IP adresu dané sítě.

2.2.6 Přijímání odpovědí

Druhé vlákno potom kontroluje příchozí zprávy a ve chvíli, kdy přijde odpověď na ARP žádost (zpráva ve které je v ARP hlavičcce v poli „operace“ 2), uloží se hodnoty IP a MAC adresy zařízení z odpovědi do pole.
Po uplynutí času 5 sekund, popřípadě po zaslání odpovídajícího signálu se zapíše mapování ve formátu XML do souboru a program končí.

2.2.7 Formát výstupu

Formát xml výstupu je následující:

```
<?xml version="1.0"?>
<!DOCTYPE devices [
<!ELEMENT devices (host+)>
<!ELEMENT host (ipv4)>
<!ELEMENT ipv4 (#PCDATA)>
<!ATTLIST host mac CDATA #REQUIRED>
]>
```

3 Použití

Program se spouští se dvěma povinými parametry, a to následovně.
`./ipk-scanner -i <jméno rozhraní> -f <výstupní soubor>`
Jméno rozhraní určuje, která síť, na kterou je zařízení připojeno bude skenována. Výstupní soubor je jméno výstupního souboru do kterého bude zapsán výstup programu ve formátu XML. Navíc je třeba jej spouštět s **právy superuživatele**.

3.1 Příklad

Příkaz:
`sudo ./ipk-scanner -i enp4s0f2 -f devices.xml`
Vypíše mapování IP adres na MAC adresy ze sítě na kterou je připojeno rozhraní `enp4s0f2` do souboru `devices.xml`.

Obsah souboru devices.xml bude například následující:

```
<?xml version="1.0"encoding="UTF-8"?>
<devices>
<host mac="0050.56ad.78ee»
<ipv4>147.229.196.2</ipv4>
</host>
<host mac="0050.5693.03cb»
<ipv4>147.229.196.3</ipv4>
</host>
</devices>
```

Reference

[1] WIKIPEDIA.ORG. *Address Resolution Protocol* [online]. 25. Březen 2017 [cit. 23. dubna 2017]. Dostupné na: <https://en.wikipedia.org/wiki/Address_Resolution_Protocol>.

[2] DIE.NET. *IOCTL(2) Linux Programmers Manual* [online]. 13. Březen 2017 [cit. 23. dubna 2017]. Dostupné na: <http://man7.org/linux/man-pages/man2/ioctl.2.html>.